

Notice of Allowability

Application No.

10/813,346

Examiner

Arezoo Sherkat

Applicant(s)

KOBAYASHI ET AL.

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 11/27/2006.
2. ☒ The allowed claim(s) is/are 23-41.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date 1/5/07 & 1/30/07.
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/27/2006 has been entered.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Michael J. Ferrazano on 1/5/2007.

The application has been amended as follows:

1-22 (Cancelled)

23. (Currently Amended) A method of using and storing a cryptography key in a display unit, comprising:

retrieving a first encrypted key from anon-volatile memory incorporated in the display unit;

generating a first decrypted key by decrypting the first encrypted key according to a first encryption protocol;

receiving a plurality of pixel data elements encoded in a display signal in an encrypted form that represents an image;

decrypting said encrypted plurality of pixel data elements using the first decrypted key;

generating said plurality of pixel data elements based upon said decrypted plurality of pixel data elements;

displaying said image on a display screen based on said decrypted plurality of pixel data elements;

destroying the first encrypted key;

receiving a second encrypted key from non-volatile memory that is different from the first encrypted key;

generating a second encrypted key by decrypting the second encrypted key according to a second encryption protocol that is different from the first encryption protocol;

decrypting said a second encrypted plurality of pixel data elements using the second decrypted key;

generating a second plurality of pixel data elements based upon said second decrypted plurality of pixel data elements;

displaying said second decrypted plurality of pixel data elements.

24. (Previously Presented) A method as recited in claim 23, wherein said display signal is received according to TMDS format.

25. (Currently Amended) ~~Computer~~ A computer program product stored on computer readable medium executable by a processor for using and storing a cryptography key in a display unit, comprising:

computer code for retrieving a first encrypted key from a non-volatile memory incorporated in the display unit;

computer code for generating a first decrypted key by decrypting the first encrypted key according to a first encryption protocol;

computer code for receiving a plurality of pixel data elements encoded in a display signal in an encrypted form that represent an image;

computer code for decrypting said encrypted plurality of pixel data elements using the first decrypted key;

computer code for generating said plurality of pixel data elements based upon said decrypted plurality of pixel data elements;

computer code for displaying said image on a display screen based on said decrypted plurality of pixel data elements;

computer code for destroying the first encrypted key;

computer code for receiving a second encrypted key from non-volatile memory that is different from the first encrypted key;

computer code for generating a second encrypted key by decrypting the second encrypted key according to a second encryption protocol that is different from the first encryption protocol;

computer code for decrypting ~~said~~ a second encrypted plurality of pixel data elements using the second decrypted key;

computer code for generating a second plurality of pixel data elements based upon said second decrypted plurality of pixel data elements;

computer code for displaying said second decrypted plurality of pixel data elements; and

a computer-readable medium for storing the computer code.

26. (Previously Presented) A method as recited in claim 23, wherein said display signal is received according to TMDS format.

27. (New) The method as recited in claim 23, further comprising receiving a cryptography-related command.

28. (New) The method as recited in claim 27, wherein the cryptography command includes an authentication request and a number of associated authentication request parameters.

29. (New) The method as recited in claim 28, wherein the authentication request is an HDCP authentication request.

30. (New) The method as recited in claim 29, further comprising:
retrieving an encrypted authentication key from the non-volatile memory
corresponding to the authentication request; and
decrypting the authentication request based upon a corresponding decryption
protocol.

31. (New) The method as recited in claim 30, further comprising:
responding to the authentication request based on the decrypted authentication request.
32. (New) Computer program product as recited in claim 25, wherein the key is one of a plurality of keys and further comprising:
computer code for providing a number of the plurality of keys.
33. (New) Computer program product as recited in claim 32, further comprising:
computer code for selecting one of the number of available encryption protocols for each of the provided keys; and
computer code for encrypting each of the provided keys based upon a particular one of the selected encryption protocols.
34. (New) Computer program product as recited in claim 33, further comprising:
computer code for storing the encrypted keys in the non-volatile memory.
35. (New) Computer program product as recited in claim 34, further comprising:
computer code for decrypting selected ones of the stored encrypted keys, as needed.
36. (New) Computer program product as recited in claim 35, wherein the plurality of keys includes a decryption key and an authentication key.
37. (New) Computer program product as recited in claim 36, further comprising:
computer code for receiving a cryptography related command.
38. (New) Computer program product as recited in claim 37 wherein the cryptography command includes an authentication request and a number of associated authentication request parameters.

39. (New) Computer program product as recited in claim 38, wherein the authentication request is an HDCP authentication request.

40. (New) Computer program product as recited in claim 39, further comprising:
computer code for retrieving an encrypted authentication key from the non volatile memory corresponding to the authentication request; and
computer code for decrypting the authentication request based upon a corresponding decryption protocol.

41. (New) Computer program product as recited in claim 40, further comprising:
computer code for responding to the authentication request based on the decrypted authentication request.

Art Unit: 2131

Allowable Subject Matter

Claim 23-41 are allowed.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

A.S.
Patent Examiner
Group 2131
Jan. 26, 2007

Taghi D. Arani
Patent Examiner
Taghi D. Arani
2/2/07